



ԱՐՄԵՆ ՀԱՐՈՒԹՅՈՒՆՅԱՆ

*ՀՀ Սահմանադրական դատարանի
նախագահի խորհրդական,
իրավունքի մագիստրոս,
քաղաքական գիտությունների
թեկնածու,
դոցենտ*



ՇՈՂԵՐ ԳՐԻԳՈՐՅԱՆ

*ՀՀ ՆԳՆ փրկարար ծառայության
կադրերի վարչության հրահանգիչ,
իրավագիտության մագիստրոս*

DOI: 10.59560/18291155-2023.1-71

**ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԻՐԱՎԱԿԱՆ
ԱՊԱՀՈՎՄԱՆ ՀԻՄՆԱԽՆԴԻՐՆԵՐԸ ԱՐՏԱԿԱՐԳ
ԻՐԱՎԻՃԱԿՆԵՐԻ ՊԱՅՄԱՆՆԵՐՈՒՄ**

Ամփոփագիր

Տեղեկատվական ոլորտը, ունենալով հասարակական կյանքը համակարգող և կարգավորող կարևոր գործառույթ, ակտիվորեն ազդում է Հայաստանի Հանրապետության (ՀՀ) անվտանգության քաղաքական, տնտեսական, ռազմական և այլ բաղադրիչների վրա: ՀՀ ազգային անվտանգությունն էականորեն կախված է տեղեկատվական անվտանգության ապահովումից, և այդ կախվածությունը մեծանում է գիտատեխնիկական առաջընթացին համընթաց: Այսօր տեղեկատվական

հոսքերը նոր բնույթի սպառնալիքներ և մարտահրավերներ են ներկայացնում պետություններին, ինչը պահանջում է տեղեկատվական դաշտում գործել այնպիսի կանոններով, որոնց մեջ վճռորոշ են տեղեկատվական հոսքերի համակարգումը, վերահսկումը և անվտանգությունը, ինչպես նաև ապատեղեկատվության տարածման և հավաստի տեղեկատվության արգելափակման միջոցով հասարակական կարծիքի խեղաթյուրման կանխարգելումը և այլն:

Այսօրինակ իրողությունների պայմաններում պետությունների անվտանգության համակարգում ռազմավարական նշանակություն է ստանում նաև պետության անվտանգության ապահովումը տեղեկատվական ոլորտում:

Սույն հոդվածը նվիրված է արտակարգ իրավիճակներում տեղեկատվական անվտանգության իրավական ապահովման հիմնահարցերի ուսումնասիրությանը: Ոլորտը կարգավորող օրենսդրության ուսումնասիրությունը թույլ է տվել բացահայտել, որ արտակարգ իրավիճակներում ՀՀ տեղեկատվական անվտանգության նորմատիվ իրավական ապահովումը՝ որպես տեղեկատվական ոլորտում ՀՀ ազգային շահերի սպառնալիքներին դիմակայելու իրավական կարգավորման միասնական համակարգ, բավարար չափով զարգացած չէ: Վեր են հանվել մի շարք հիմնահարցեր, որոնց կարգավորումը հնարավոր կդառնա օրենսդրական բարեփոխումների արդյունքում:

Հիմնաբառեր. ազգային շահեր, տեղեկատվական անվտանգություն, արտակարգ իրավիճակներ, տեղեկատվական սպառնալիքներ, իրավական ապահովում, հիմնահարցեր, ռազմավարություն:

Տեղեկատվական անվտանգությունն ազգային անվտանգության անբաժանելի մասն է կազմում: Դա պայմանավորված է նրանով, որ տեղեկատվությունը բոլոր ժամանակներում առանցքային դեր է ունեցել պետության կայունության և անվտանգության ապահովման հարցում:

Անվտանգություն հասկացությունը, թվացյալ պարզության հետ մեկտեղ, խիստ ընդգրկուն է և գործնականորեն ներառում է հասարակության ու առանձին անհատների կենսագործունեության բոլոր ոլորտները:

Անվտանգության փիլիսոփայության ստեղծման գործում մեծ ավանդ ունի անգլիացի պատմաբան, փիլիսոփա Առնոլդ Թոյնբին: Եթե ուսում-

1(109)2023
ՏԵՂԵԿՎՈՐՈՒՄԻ ՆՅՈՒԹԵՐ

նասիրենք և ընդհանրացնենք Թոյնբիի դասական մոտեցումները, ձևակերպումները անվտանգության վերաբերյալ, ապա կարող ենք ասել, որ քաղաքակրթությունների, պետությունների, հասարակությունների և անգամ անհատների անվտանգությունն ապահովվում է նրանց՝ մարտահրավերների և դրանց տրվող պատասխանների բարդ համակարգում գործելու ունակությամբ: Հայտնի է Թոյնբիի ասույթը, թե քաղաքակրթությունների կործանման պատճառը եղել է նրանց անկարողությունը՝ ադեկվատ արձագանքելու իրենց նետված մարտահրավերներին: Նկատենք, սակայն, որ մարտահրավերները որոշ իրադրություններում կարող են ընկալվել նաև որպես դրական հանգամանք, քանի որ դրանք ստուգում, փորձաքննում են անվտանգության համակարգի հուսալիությունը և, մարտահրավերներին արժանիորեն դիմագրավելու նպատակով, մոբիլիզացնում են հանրության հոգևոր, մտավոր, ռազմաքաղաքական ու նյութական ռեսուրսները: Թոյնբիի վերոնշյալ դատողությունները կիրառելի են նաև տեղեկատվական անվտանգության ոլորտում¹:

Տեղեկատվական անվտանգության ապահովումն առավել քան կարևոր նշանակություն է ձեռք բերում արտակարգ իրավիճակներում, որտեղ տեղեկատվական ազդեցությունը կարող է ֆիզիկական, նյութական և բարոյական վնաս հասցնել անհատին, հասարակությանը, պետությանը, առաջացնել մարդկանց կամ անհատների տարբեր խմբերի ոչ համարժեք սոցիալական կամ հանցավոր վարք և բացահայտել պետության ենթակառուցվածքների թույլ ու խոցելի կետերը:

Ժամանակակից պայմաններում, արտակարգ իրավիճակներում ՀՀ ազգային անվտանգության, ազգային շահերի անվտանգության ապահովումը տեղեկատվական ոլորտում ենթադրում է հարաբերությունների իրավական կարգավորման համակարգի առաջնահերթ զարգացում, սպառնալիքներին հակազդելու և դրանք կարգավորելու նպատակով համապատասխան օրինաստեղծ գործընթաց:

Վերոնշյալ գործընթացն առաջին հերթին պայմանավորված է նրանով, որ իրավական պետության և քաղաքացիական հասարակության կառուցման պայմաններում ազգային անվտանգության համար պատասխանատու պետական մարմինների գործունեությունը պետք է կարգավորվի որո-

¹ Տե՛ս **Հարությունյան Գ.Ա.**, Տեղեկատվական անվտանգություն: Եր., «Նորավանք» ԳԿՀ, 2017, էջ 102:

շակի իրավական նորմերով, որոնք ապահովում են մարդու և քաղաքացու սահմանադրական իրավունքների և ազատությունների իրականացումը:

Երկրորդ՝ ոլորտում օրենսդրության ընդունումն ուղղված է ՀՀ ազգային անվտանգությանն սպառնացող վտանգների հակազդելու նպատակների նորմատիվային ամրագրմանը, դրանց հասնելու միջոցներին և մեթոդներին, իշխանությունների համակարգված գործունեության ապահովմանը:

Երրորդ՝ ՀՀ ինտեգրումը միջազգային հանրությանը զգալիորեն ընդլայնում է երկրի տեղեկատվական անվտանգության ամրապնդման հնարավորությունները՝ միջազգային իրավունքի մշակմանը մասնակցության, տեղեկատվական ոլորտի անվտանգության ապահովման միջազգային համակարգի ստեղծման միջոցով:

Արտակարգ իրավիճակներում տեղեկատվական անվտանգության իրավական ապահովումն ստեղծվում է արտակարգ իրավիճակներում ՀՀ տեղեկատվական անվտանգության ապահովման իրավական կարգավորման համակարգի և այս համակարգի ձևավորման գործընթացի համադրությամբ: Արտակարգ իրավիճակներում տեղեկատվական անվտանգության իրավական կարգավորման համակարգն իր հերթին ներառում է ոլորտում հարաբերությունները կարգավորող իրավական նորմերը և դրանց կիրառումից բխող իրավահարաբերությունները:

Իրավական նորմերը հիմք են հանդիսանում արտակարգ իրավիճակներում տեղեկատվական անվտանգության ապահովման համար և մեծապես որոշում են պետության, հասարակության և առանձին քաղաքացիների գործունեության արդյունավետությունը տեղեկատվական ոլորտում պետության ազգային շահերը պաշտպանելու գործում¹:

Մինչույն ժամանակ, օրինաստեղծ գործընթաց իրականացնելու համար նախ անհրաժեշտ է դիտարկել ՀՀ տեղեկատվական անվտանգության մարտահրավերները, ինչպես նաև արտակարգ իրավիճակներում տեղեկատվական անվտանգության իրավական ապահովման հիմնահարցերը:

¹ Чеботарева А.А. Информационное право: учебное пособие. - М.: Юридический институт МИИТ, 2014. - С .160.

«Վ ազգային անվտանգության խորհրդի կողմից 2020 թվականի հուլիսի 10-ին ընդունված «Վ ազգային անվտանգության ռազմավարության մեջ ներդրված են «Վ տեղեկատվական անվտանգության ապահովման կարևորագույն խնդիրները:

-տեղեկատվական և կիբեռանվտանգության ոլորտը կարգավորող համապարփակ պետական քաղաքականության անկատարությունը,

-կենսական նշանակության տեղեկատվական ենթակառուցվածքների պաշտպանությունն ապահովող օրենսդրության բացակայությունը,

-համակարգչային պատահարների արձագանքման կառույցների ինստիտուցիոնալ կարողությունների ոչ բավարար մակարդակը,

-կիբեռանվտանգության ոլորտը համակարգող կառույցի բացակայությունը¹:

Ռազմավարության մեջ տեղ չեն գտել 2009 թվականի «Վ տեղեկատվական անվտանգության հայեցակարգում ամրագրված մի շարք խնդիրներ: Մասնավորապես, տեղեկատվական տիրույթում միջազգային համագործակցության ոչ բավարար մակարդակը, «Վ տեղեկատվական անվտանգության ապահովման իրավական նորմատիվային բազայի բարելավումը, ներառյալ՝ տեղեկատվություն ստանալու քաղաքացիների իրավունքների իրականացման մեխանիզմների և զանգվածային լրատվամիջոցների հետ պետության փոխհարաբերությունը կարգավորող իրավական նորմերի կատարելագործումը, տեղեկատվական անվտանգության պահանջների պահպանման գործում պետական իշխանության և տեղական ինքնակառավարման մարմինների պաշտոնատար անձանց, իրավաբանական անձանց և քաղաքացիների պատասխանատվության սահմանումը, «Վ տեղեկատվական անվտանգության ապահովման նպատակային պետական ծրագրերի մշակումը, տեղեկատվության պաշտպանության և պետական գաղտնիքի պաշտպանության պետական համակարգերի զարգացումը և կատարելագործումը, տեղեկատվության պաշտպանության ժամանակակից մեթոդների և միջոցների մշակումը, տեղեկատվական տեխնոլոգիաների անվտանգության ապահովումն առաջին հերթին զինված ուժերի, բնապահպանական տեսանկյունից վտանգավոր և հատուկ կարևորություն ունեցող արտադրությունների կառավար-

¹ Տե՛ս «Վ ազգային անվտանգության ռազմավարություն, «Վ ազգային անվտանգության խորհրդի 10.07.2020թ. որոշում:

ման համակարգերում, խաղաղ պայմաններում, արտակարգ իրավիճակներում և պատերազմական ժամանակ պետության կառավարման ժամանակակից պաշտպանված տեխնոլոգիական հիմքերի ստեղծումը ու զարգացումը և մի շարք այլ հիմնախնդիրներ¹:

Հարկ է նշել, որ վերոնշյալ հիմնախնդիրները շարունակում են դեռևս արդիական մնալ:

Ներկայումս, արտակարգ իրավիճակներում ՀՀ տեղեկատվական անվտանգության նորմատիվ իրավական ապահովումը՝ որպես տեղեկատվական ոլորտում ՀՀ ազգային շահերի սպառնալիքներին դիմակայելու իրավական կարգավորման միասնական համակարգ, բավարար չափով զարգացած չէ:

Օրինաստեղծ գործընթացում կան որոշակի բացթողումներ: Օրենսդրությունն այս ոլորտում բնութագրվում է քառսային և մասնատված նախաձեռնություններով:

Դիտարկենք իրավական ապահովման առանցքային հիմնահարցերից մի քանիսը:

Արտակարգ իրադրությունների, ճգնաժամային իրավիճակների, պատերազմական գործողությունների ընթացքում ապատեղեկատվության ծավալները կտրուկ աճում են, ինչը դժվարեցնում է հանրության շրջանում խուճապային տրամադրությունների, կեղծ տեղեկատվական հոսքերի կառավարելիությունը:

Չնայած ապատեղեկատվության լայն տարածվածությանը՝ ՀՀ-ում դեռևս հաստատված չէ ապատեղեկատվության դեմ պայքարի ռազմավարական որևէ փաստաթուղթ: Ապատեղեկատվության դեմ պայքարի ռազմավարության բացակայության պատճառով ՀՀ հասարակությունը մնում է անտեղյակ և խոցելի տեղեկատվական վակուումը լրացնող կեղծ պատմույթների հանդեպ²:

¹ Տե՛ս «ՀՀ տեղեկատվական անվտանգության հայեցակարգը հաստատելու մասին» ՀՀ Նախագահի ՆԿ-97-Ն կարգադրություն (26.06.2009 թ. ուժի մեջ է մտել 25.07.2009 ՀՀՊՏ 2009.07.15/35(701) Հոդ.820):

² Տե՛ս Freedom House, Disinformation and misinformation in Armenia confronting the power of false narratives, 2021թ., [Disinformation-in-Armenia_Am-final.pdf \(freedomhouse.org\)](https://www.freedomhouse.org/sites/default/files/2021-07/Disinformation-in-Armenia_Am-final.pdf), էջ 14:

Ապատեղեկատվության դեմ պայքարի ամենաարդյունավետ միջոցներից մեկը կառավարման համակարգում պրոակտիվ հրապարակայնության մակարդակի բարելավումն է և բազմակողմ հաղորդակցությունը¹:

Պրոակտիվ հրապարակայնության էությունն այն է, որ պետական մարմինները սեփական նախաձեռնությամբ հրապարակում են իրենց գործունեությանն առնչվող տեղեկատվություն՝ մատչելիության, արդիակայնության և ամբողջականության սկզբունքների հիման վրա²:

Պետական գերատեսչությունները պետք է միջոցառումներ ձեռնարկեն հանրային հետաքրքրության պաշտոնական փաստաթղթերը լիարժեք հանրայնացնելու ուղղությամբ ինչպես իրենց նախաձեռնությամբ, այնպես էլ հարցման հիման վրա, որպեսզի նպաստեն բաց և արդյունավետ կառավարմանը և կանխեն կեղծ տեղեկությունների ի հայտ գալը:

Այս համատեքստում օրենսդրական դաշտի բացերից է նաև հանրային իրազեկման ոլորտը կարգավորող օրենսդրության բացակայությունը, ինչը նույնպես խթանում է ապատեղեկատվության տարածմանը:

Ոլորտը կարգավորող օրենսդրության մյուս խնդիրներից է տեղեկատվական անվտանգության ապահովման նպատակների, խնդիրների, սկզբունքների և հիմնական ուղղությունների նկատմամբ պետության պաշտոնական մոտեցումները ներկայացնող փաստաթղթի՝ տեղեկատվական անվտանգության հայեցակարգի բացակայությունը:

2017 թվականին ՀՀ նախագահի ՆԿ-145-Ն կարգադրությամբ ՀՀ տեղեկատվական անվտանգության հայեցակարգն ուժը կորցրած ճանաչվեց, ինչը պայմանավորված էր նրանով, որ Կառավարությունը նախապատրաստվում էր մշակել և հաստատել ոլորտի նոր ռազմավարություն: Ինչպես և նախորդ հայեցակարգը, ՀՀ տեղեկատվական անվտանգության ապահովման և տեղեկատվական քաղաքականության ռազմավարության նախագիծը ներառում էր նաև հանրային կենսագործունեության տարբեր ոլորտներում, այդ թվում՝ արտակարգ իրավիճակներում տեղեկատվական անվտանգության ապահովման հիմնական ուղղությունները և

¹ Տե՛ս Ապատեղեկատվության դեմ պայքարի ռազմավարության նախագիծ 2023-2025, http://www.foi.am/u_files/file/DOCS%202022/Strategy-against-Disinformation-Final-ARM-2023-2025.pdf

² Տե՛ս Պրոակտիվ հրապարակման ապահովումը պաշտոնական ինտերնետային կայքերում, http://www.foi.am/u_files/file/E-FOI_monitoring.pdf

ակնկալվող գործողությունները¹: Նույն թվականին մշակվեց նաև ՀՀ կիբեռանվտանգության ռազմավարության նախագիծը, որը նախատեսում էր Կիբեռանվտանգության կենտրոնի ստեղծում²:

Թեև երկու ռազմավարություններն էլ առանցքային նշանակություն ունեն ոլորտում օրենսդրության բարելավման և արդիականացման համար, սակայն դրանք առ այսօր չեն հաստատվել:

Մյուս կարևոր հիմնահարցերից է մեդիագրագիտությունը: Մեդիագրագիտության տարածման աշխատանքը համակարգելու համար եվրոպական մի շարք երկրներ (Ֆինլանդիա, Մեծ Բրիտանիա³, Շվեդիա), կարևորելով մեդիագրագիտության դերը, ներդրել են մեդիագրագիտության ապահովման կառույց, որը նաև հետևում է մեդիայի աշխատանքին և համապատասխան օրենսդրության պահպանությանը լրատվամիջոցներում:

Մեդիագրագիտության տարածման միջազգային լավագույն փորձը հուշում է նաև, որ այս գործընթացը պետք է հիմնված լինի խորը հետազոտությունների ու տվյալների վրա, ունենա մանրամասն մշակված ռազմավարություն և գործողությունների ծրագիր, լինի համընդգրկուն, համակարգային և շարունակական⁴:

Տեղեկատվական անվտանգության իրավական ապահովման վերոնշյալ հիմնահարցերը զգալիորեն նվազեցնում են տեղեկատվական ոլորտում ՀՀ ազգային շահերի պաշտպանությունը:

Նշված թերությունները վերացնելու համար անհրաժեշտ է նպատակաուղղված գործունեություն ծավալել երկրի տեղեկատվական անվտանգության իրավական ապահովման բարելավման ուղղությամբ:

Մինևնույն ժամանակ, տեղեկատվական անվտանգության ապահովման իրավական մեխանիզմների համակարգը պետք է խարսխված լինի

¹ Տե՛ս Նախագահ Սերժ Սարգսյանը հրավիրել է Ազգային անվտանգության խորհրդի նիստ

<https://www.president.am/hy/press-release/item/2017/09/27/President-convened-National-Security-Council-meeting/>

² Տե՛ս Կիբեռանվտանգության ռազմավարությունը հաստատելու մասին ՀՀ կառավարության որոշման նախագիծ <https://www.e-draft.am/projects/581/about>

³ Տե՛ս Department for Digital, Culture, Media and Sport, UK, Online Media Literacy Strategy, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004233/DCMS_Media_Literacy_Report_Roll_Out_Accessible_PDF.pdf

⁴ Տե՛ս Finnish Ministry of Education and Culture, Media Literacy in Finland: national media education policy, 2019, <https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf>

1(109)2023

◆ ՏԵՂԵԿՎՈՐ

◆ ՍԱՀՄԱՆԱՐՈՎԱԿԱՆ ՂԱՏԱՐԱՆ

անհատի, հասարակության և պետության շահերի համադրման սկզբունքով: Անհատի, հասարակության և պետության շահերի հավասարակշռությունը որոշելիս անհրաժեշտ է ելնել նաև այն հանգամանքից, որ ՀՀ-ն հանդիսանում է ինքնիշխան, ժողովրդավարական, իրավական և սոցիալական պետություն, որի պարտականությունն է մարդու իրավունքների և ազատությունների ճանաչումը, դրանց պահպանության, ապահովման և պաշտպանության համար երաշխիքների ստեղծումը, մարդու (քաղաքացու) արժանապատիվ կյանքի և ազատ զարգացման պայմանների ստեղծումը և ապահովումը, ՀՀ ազգային անվտանգությանը սպառնացող վտանգների չեզոքացումը:

Օգտագործված նորմատիվ իրավական ակտերի և գրականության ցանկ

1. «ՀՀ տեղեկատվական անվտանգության հայեցակարգը հաստատելու մասին» ՀՀ Նախագահի ՆԿ-97-Ն կարգադրություն (26.06.2009 թ. ուժի մեջ է մտել 25.07.2009 ՀՀ ՊՏ 2009.07.15/35(701) հոդվ.820):
2. ՀՀ ազգային անվտանգության ռազմավարություն, ՀՀ ազգային անվտանգության խորհրդի 10.07.2020 թ. որոշում:
3. Ապատեղեկատվության դեմ պայքարի ռազմավարության նախագիծ 2023-2025 http://www.foi.am/u_files/file/DOCs%202022/Strategy-against_Disinformation-Final-ARM-2023-2025.pdf
4. Կիբեռանվտանգության ռազմավարությունը հաստատելու մասին ՀՀ կառավարության որոշման նախագիծ <https://www.e-draft.am/projects/581/about>
5. **Հարությունյան Գ.Ա.**, Տեղեկատվական անվտանգություն, Եր.: «Նորավանք» ԳԿՀ, 2017, 320 էջ:
6. **Чеботарева А.А.** Информационное право: учебное пособие. - М.: Юридический институт МИИТ, 2014. - С. 160.
7. Նախագահ Սերժ Սարգսյանը հրավիրել է Ազգային անվտանգության խորհրդի նիստ <https://www.president.am/hy/press-release/item/2017/09/27/President-convened-National-Security-Council-meeting/>
8. Պրոակտիվ հրապարակման ապահովումը պաշտոնական ինտերնետային կայքերում http://www.foi.am/u_files/file/E-FOI_monitoring.pdf

9. Freedom House, Disinformation and misinformation in Armenia confronting the power of false narratives, 2021թ., [Disinformation-in-Armenia Am-final.pdf \(freedomhouse.org\)](#), p. 14.

10. Department for Digital, Culture, Media and Sport, UK, Online Media Literacy Strategy, 2021, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004233/DCMS Media Literacy Report Roll Out Accessible PDF.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004233/DCMS_Media_Literacy_Report_Roll_Out_Accessible_PDF.pdf)

11. Finnish Ministry of Education and Culture, Media Literacy in Finland: national media education policy, 2019, <https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf>

ПРОБЛЕМЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

Аннотация

Информационная сфера, выполняя важную функцию координации и регулирования общественной жизни, активно влияет на политическую, экономическую, военную и другие составляющие безопасности Республики Армения (РА). Национальная безопасность РА в значительной степени зависит от обеспечения информационной безопасности, и эта зависимость возрастает вместе с научно-техническим прогрессом. Сегодня информационные потоки представляют угрозы и вызовы нового характера для государств, что требует действовать в информационном поле по таким правилам, при которых обеспечивается координация, контроль и безопасность информационных потоков, а также недопущение искажения общественного мнения путем распространения ложной информации и блокирования достоверной информации и т. д.

В условиях таких реалий в системе безопасности государств стратегическое значение приобретает и обеспечение безопасности государства в информационной сфере.

Данная статья посвящена исследованию проблемных вопросов правового обеспечения информационной безопасности в чрезвычайных ситуациях.

Изучение законодательства, регулирующего отрасль, позволило выявить, что нормативное правовое обеспечение информационной безопасности РА в условиях чрезвычайных ситуаций как единая система согласованных норм правового регулирования отношений в области противодействия угрозам национальных интересов РА в информационной сфере развито недостаточно. Были подняты вопросы, решение которых заключается в совершенствовании законодательства.

Ключевые слова. национальные интересы, информационная безопасность, чрезвычайные ситуации, информационные угрозы, правовое обеспечение, основные вопросы, стратегия.

THE PROBLEMS OF LEGAL PROVISION OF INFORMATION SECURITY IN EMERGENCY SITUATIONS

Annotation

Information sphere, performing an important function of coordination and regulation of public life, actively influences the political, economic, military and other components of the security of the Republic of Armenia (RA). The national security of the Republic of Armenia largely depends on the provision of information security, and this dependence is increasing along with scientific and technical progress. Today, information flows pose threats and challenges of a new nature for states, which requires action in the information field with such rules that ensure coordination, control and security of information flows, as well as prevention of distortion of public opinion by spreading false information and blocking reliable information and etc.

In such realities information security acquires strategic importance in the security system of the state.

This article is devoted to the study of issues of legal provision of information security in emergency situations.

The study of the legislation regulating the sector allowed to reveal, that the normative legal provision of the information security in emergency situations

in RA as an entire system for the protection of the national interests of RA is not sufficiently developed. The way of the settlement of the raised issues passes through the improvement of the legislation.

Keywords: national interests, information security, emergencies, information threats, legal provision, main issues, strategy.

Հոդվածը հանձնված է խմբագրություն 13.03.2023, տրվել է գրախոսության 14.03.2023, ընդունվել է տպագրության 20.03.2023:

